UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

BELINDA GULLETTE and **LAWRENCE BURGER**, on behalf of themselves and all others similarly situated, Plaintiffs, v. **WEBTPA EMPLOYER SERVICES, LLC**, Defendant.	No. 3:24-cv-01160 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Belinda Gullette and Lawrence ("Larry") Burger (together "Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against WebTPA Employer Services, LLC ("WebTPA" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a third-party insurance administrator that serves clients in industries across the nation, including automotive, health, hospitality, finance, and municipalities.[1] WebTPA

[1] *WebTPA,* WEBTPA, https://www.webtpa.com/ (last visited May 14, 2024).

serves over 2.7 million members with 25,000 benefit plan structures, resulting in over 6.4 million claims processed annually.[2]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former consumers. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. On information and belief, the Data Breach began on April 18, 2023, when an unauthorized party gained access to WebTPA's network, and lasted until at least April 23, 2023 – providing cybercriminals unfettered access to WebTPA's former and current customers' highly private information for an entire week. The Data Breach was not discovered by WebTPA until eight months later, on December 28, 2023.

5. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former consumers' PII.

6. Following an internal investigation, WebTPA learned cybercriminals had gained unauthorized access to WebTPA's customers' personally identifiable information ("PII") including but not limited to name, contact information, date of birth, date of death, Social Security number, and insurance information.[3]

7. WebTPA's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its employees how many people were impacted, how the breach happened,

[2] *A History of Innovative Service,* WEBTPA, https://www.webtpa.com/webtpahistory (last visited May 14, 2024).
[3] *Notice of Data Security Incident*, WEBTPA, https://www.webtpa.com/notice (last visited May 14, 2024).

or why it took the WebTPA over a year to begin notifying victims that hackers had gained access to highly sensitive PII.

8. Defendant's failure to timely detect and report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former employees.

11. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

12. Plaintiffs are Data Breach victims, having received breach notices. *See example* of a Data Breach Notice (Exhibit A). They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

13. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former consumers' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

14. Plaintiff, Belinda Gullette, is a natural person and citizen of Ohio. She resides in Cincinnati, Ohio here she intends to remain.

15. Plaintiff, Larry Burger, is a natural person and citizen of Oklahoma. He resides in Alva, Oklahoma where he intends to remain.

16. Defendant, WebTPA Employer Services, LLC, is a domestic company formed in Texas with its principal place of business at 8500 Freeport Pkwy South, Suite 400, Irving Texas 75063. Defendant is a citizen of Texas. The registered agent for service of process is Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Both Plaintiffs, Belinda Gullette and Larry Burger, and Defendant are citizens of different states. And there are over 100 putative Class members.

18. This Court has personal jurisdiction over Defendant because its headquarters and principal place of business is located in the Dallas Division of the Northern District of Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

19. Venue is proper in this Court because Defendant's principal office is in the Dallas Division of the Northern District of Texas, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiffs and the Class

20. Defendant is a third-party insurance administrator that serves clients in industries across the nation, including automotive, health, hospitality, finance, and municipalities.[4] WebTPA serves over 2.7 million members with 25,000 benefit plan structures, resulting in over 6.4 million claims processed annually.[5]

21. As part of its business, Defendant receives and maintains the PII of thousands of its current and former customers.

22. On information and belief, WebTPA was provided with Plaintiffs' PII as part of the administration services WebTPA provides to insurance and benefits providers.

23. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their PII.

24. Under state and federal law, businesses like Defendant have duties to protect its current and former consumers' PII and to notify them about breaches.

25. Defendant recognizes these duties, declaring in its "Privacy Statement" that:

a. "In general, we may collect personal information about you, directly and indirectly, depending on your relationship with us -- whether as an individual client, agent, broker, a policyholder, claimant, employee of our

[4] *WebTPA,* WEBTPA, https://www.webtpa.com/ (last visited May 14, 2024).
[5] *A History of Innovative Service,* WEBTPA, https://www.webtpa.com/webtpahistory (last visited May 14, 2024).

clients, family member of any such person, or other person who we employ or with whom we do business."[6]

b. "The information WebTPA may obtain includes, but is not limited to, your past, present, or future physical or mental health or condition, the provision of health care to you, payment for the provision of health care to you, your Social Security number, employment history, credit history, income information, and bank or credit card information, date of birth, gender, race/national origin, contact details (home and work address, telephone numbers, email addresses), and username, password, password reminder questions and answers for WebTPA Online Services."[7]

c. "WebTPA has implemented physical, electronic and technical safeguards to protect your personal information, consistent with applicable privacy and data security laws."[8]

d. "We will securely delete or erase your personal information if there is no valid business reason for retaining that information."[9]

e. "We do not sell any of your personal information to third parties."[10]

Defendant's Data Breach

26. The Data Breach began on April 18, 2023, when an unauthorized party gained access to WebTPA's network, and lasted until at least April 23, 2023 – providing cybercriminals

[6] *WebTPA Privacy Statement*, WEBTPA, https://www.webtpa.com/privacy (last visited May 14, 2024).
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*

unfettered access to WebTPA's former and current customers' highly private information for almost an entire week.

27. The Data Breach was not detected by WebTPA until eight months later, on December 28, 2023.

28. Additionally, Defendant admitted that PII was actually stolen during the Data Breach confessing that the information was not just accessed, but that the "unauthorized actor may have accessed and/**or obtained** personal information." Ex. A

29. Because of Defendant's Data Breach, at least the following types of PII were compromised:

a. names;

b. contact information;

c. dates of birth;

d. dates of death

e. Social Security numbers; and

f. insurance information.[11]

30. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former consumers.

31. And yet, Defendant waited over until May 8, 2024, before it began notifying the class—over an entire year after the Data Breach began.

[11] *Notice of Data Security Incident*, WEBTPA, https://www.webtpa.com/notice (last visited May 14, 2024).

32. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

33. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing credit reports and Explanations of Benefits ("EOBs") from your benefit plans for suspicious activity;"

b. "[i]f you identify suspicious activity, you should contact the entity that maintains the information on your behalf;"

c. [y]ou may want to consider placing a fraud alert on your credit file;"

d. "[y]ou have the right to place a security freeze on your credit free of charge;" and

e. "[i]f you are the victim of fraud or identity theft, you also have the right to file a police report." Ex. A.

34. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

35. Since the breach, Defendant promises that it "deployed additional security measures and tools… to further strengthen the security of [its] network." Ex. A.

36. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

37. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

38. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

39. Defendant has done little to remedy its Data Breach. True, Defendant has offered victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Defendant inflicted upon them.

Plaintiff Belinda Gullette's Experiences and Injuries

40. Plaintiff Belinda Gullette is a former customer of Defendant—having received life and accident insurance from a company that receives administration services from Defendant.

41. Thus, Defendant obtained and maintained Plaintiff's PII.

42. As a result, Plaintiff was injured by Defendant's Data Breach.

43. As a condition of receiving insurance services, Plaintiff was required to provide Defendant or its third-party agents with her PII. Defendant used that PII to facilitate its provision of insurance administration services and to collect payment.

44. Plaintiff provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

45. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

46. Plaintiff received a Notice of Data Breach on May 14, 2024.

47. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

48. Through its Data Breach, Defendant compromised Plaintiff's:

a. name;

b. contact information;

c. date of birth; and

d. Social Security number.

49. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect themselves from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

50. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

51. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

52. Plaintiff suffered actual injury from the exposure and theft of her PII—which violates his rights to privacy.

53. And in the aftermath of the Data Breach, Plaintiff has suffered from a dramatic spike in spam and scam phone calls and emails.

54. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

55. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

56. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

57. Today, Plaintiff has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Larry Burger's Experiences and Injuries

58. Plaintiff Larry Burger is not associated with WebTPA and is unsure how Defendant acquired his PII.

59. Plaintiff Burger received a notice from Defendant on or around May 14, 2024, stating that his PII was involved in the Data Breach including his name and Social Security number.

60. At the time of the Data Breach, Defendant retained Plaintiff Burger's PII in its system.

61. Plaintiff trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

62. Plaintiff Burger is very careful about sharing and protecting his Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

63. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

64. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

65. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

66. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

67. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

68. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

69. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

70. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

71. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

72. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

73. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

74. The value of Plaintiffs and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

75. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

76. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

77. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

78. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class members, and it is reasonable for any trier of fact, including this

Court or a jury, to find that Plaintiffs and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

79. Defendant disclosed the PII of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

80. Defendant's failure to promptly and properly notify Plaintiffs and Class members of the Data Breach exacerbated Plaintiffs and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

81. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

82. According to the 2023 Annual Data Breach Report, the number of data compromises in 2023 (3,205) increased by 78 percentage points compared to 2022 (1,801). The ITRC set a new record for the number of data compromises tracked in a year, up 72 percentage points from the previous all-time high in 2021 (1,860).[12]

83. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware

[12] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://www.idtheftcenter.org/publication/2023-data-breach-report/

of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

84. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

85. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

86. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[14] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

[13] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited May 15, 2024).

[14] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

87. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

88. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

89. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

90. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former consumers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

91. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

92. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

93. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

94. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

95. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by WebTPA Employer Services in December 2023, including all those individuals who received notice of the breach.

96. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any

successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

97. Plaintiffs reserve the right to amend the class definition.

98. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

99. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

100. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 100 members.

101. Typicality. Plaintiffs' claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

102. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

103. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

104. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device

provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

105. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

106. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

107. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

108. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if their PII was wrongfully disclosed.

109. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' PII.

110. Defendant owed—to Plaintiffs and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII.

111. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

112. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

113. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

114. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

115. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold vast amounts of PII, it was inevitable that

unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

116. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class members' and the importance of exercising reasonable care in handling it.

117. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

118. Defendant breached these duties as evidenced by the Data Breach.

119. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

120. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs and Class members' injury.

121. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class members' injuries-in-fact.

122. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

123. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

124. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

125. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

126. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

127. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC

publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' sensitive PII.

129. Defendant breached its respective duties to Plaintiffs and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

130. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

131. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

132. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class members would not have been injured.

133. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

134. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

135. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

136. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

137. Plaintiff and Class members either directly contracted with Defendant or Plaintiff and Class members were the third-party beneficiaries of contracts with Defendant.

138. Plaintiffs and Class members were required to provide their PII to Defendant as a condition of receiving insurance services provided by Defendant or its third-party agents. Plaintiffs and Class members provided their PII to Defendant or its third-party agents in exchange for Defendant's administrative insurance services.

139. Plaintiffs and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

140. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

141. Plaintiffs and the Class members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for insurance services.

142. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

143. In its Privacy Statement, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII.

144. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

145. After all, Plaintiffs and Class members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

146. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

147. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

148. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

149. Defendant materially breached the contracts it entered with Plaintiffs and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

150. In these and other ways, Defendant violated its duty of good faith and fair dealing.

151. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

152. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

153. Plaintiffs and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

154. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

155. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

156. Defendant owed a duty to its current and former consumers, including Plaintiffs and the Class, to keep this information confidential.

157. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' PII is highly offensive to a reasonable person.

158. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did

so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

159. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

160. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

161. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

162. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

163. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

164. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

165. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

166. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

167. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

169. This claim is pleaded in the alternative to the breach of implied contract claim.

170. Plaintiffs and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII to facilitate its provision of services, and (2) receiving payment from Plaintiffs and Class members.

171. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members.

172. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

173. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII.

174. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

175. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' PII and/or payment because Defendant failed to adequately protect their PII.

176. Plaintiffs and Class members have no adequate remedy at law.

177. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

178. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

179. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

180. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

181. Because of the highly sensitive nature of the PII, Plaintiffs and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

182. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII.

183. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

184. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: May 15, 2024

Respectfully submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214/744-3000 / 214/744-3015 (fax)
jkendall@kendalllawgroup.com

STRAUSS BORRELLI LLP
Samuel J. Strauss*
Raina Borrelli*
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro hac vice forthcoming*
Attorneys for Plaintiffs and the Proposed Class